Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

Nr. 7 (174) / 2020
Indexat în
CEEOL și ROAD

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

ORGANIZAȚIILE INTERNAȚIONALE ȘI BUNELE PRACTICI ÎN DOMENIUL SECURITĂȚII CIBERNETICE

Tasia GUDU

International organizations and the good practices in cybersecurity
Abstract: *The good practices are considered an indicator of the activity performed by the international organizations. This article aims to show the interaction between international organizations and states in testing the practices over a period of time and the results that are validating them as successful. In the cybersecurity domain, the use of best practices by the states makes them more aware of the threats, of the possible responses and the risks. Generally, the use of best practices aims to confirm the coordination role of the international organizations and to legitimate their activity.*
Keywords: *good practices, international organizations, ENISA, incident reporting, cybersecurity.*

Organizațiile internaționale și bunele practici în domeniul securității cibernetice
Rezumat: *Bunele practici sunt considerate un indicator al activității organizațiilor internaționale. Acest articol are ca obiectiv să prezinte interacțiunea dintre organizații internaționale și state în testarea practicilor pe o anumită perioadă și rezultatele ce validează aceste practici ca fiind de succes. În domeniul securității cibernetice, aplicarea bunelor practici de către state are ca efect o conștientizare crescută a riscurilor și amenințărilor și a metodelor de răspuns. În general, utilizarea bunelor practici confirmă rolul coordonator al organizațiilor internaționale și legitimează activitatea acestora.*
Cuvinte-cheie: *bune practici, organizații internaționale, ENISA, raportarea incidentelor, securitate cibernetică.*

Introducere

Pandemia curentă a favorizat reflecția asupra gradului în care organizațiile internaționale sunt pregătite să răspundă unei crize ce afectează statele în mod simultan. Contestarea rolului organizațiilor internaționale face chiar subiectul articolelor de presă în această perioadă, ceea ce lasă să se întrevadă anvergura crizei pe care o traversează organismele respective. Trebuie menționat că acest tip de criză, cu extindere transfrontalieră rapidă, ajută la înțelegerea altor provocări cu care se confruntă statele, precum securitatea cibernetică, care împărtășesc anumite caracteristici.

Sunt organizațiile internaționale pregătite să mențină o comunicare eficientă cu statele în cazul unei crize ce ar afecta simultan infrastructurile lor de comunicații? Ce indicatori pot evidenția activitățile desfășurate de organizațiile internaționale, tipurile de interacțiune cu statele sau rezultatele obținute? Pentru a răspunde la aceste întrebări, rapoartele generate de organizațiile internaționale reprezintă, de cele mai multe ori, principala sursă de documentare și cunoaștere. Dar, modalitatea în care acestea sunt întocmite sau datele care stau la baza lor sunt adeseori contestate. Acesta este cadrul în care am considerat analiza practicilor inițiate de organizațiile internaționale în domeniul securității cibernetice ca indicator al modului de funcționare și al rolului acestor instituții, al tipului de interacțiune cu statele și al metodologiilor folosite pentru colectarea datelor.

Implementarea practicilor reprezintă modalitatea prin care statele sunt angajate într-o interacțiune regulată cu organizațiile internaționale, la baza căreia se află un canal de comunicare duplex între actorii respectivului context multilateral. În documentele emise de aceste organisme, termenul este foarte des utilizat în sintagma „bune practici”, care pune sub semnul întrebării procesul și condițiile prin care practicile din cadrul organizațiilor internaționale sunt validate ca fiind potrivite pentru a fi aplicate

***Tasia GUDU** este doctorand în domeniul Științe politice (relații internaționale) în cadrul Școala Națională de Studii Politice și Administrative (e-mail: gudutasia@yahoo.com).*

de către state. Potrivit unei definiții generice a bunelor practici propusă Agenția ONU pentru alimentație și agricultură, acestea reprezintă experiențe ce pot fi recomandate ca model, după o testare și aplicare prealabilă în diferite contexte[1]. În domeniul securității cibernetice, acest concept este frecvent vehiculat în contextul cooperării dintre actori și are ca obiectiv procesul de învățare între state cu grad diferit de maturitate a strategiilor naționale de securitate cibernetică. Diferite organizații internaționale propun proceduri și metodologii sau realizează studii care au ca scop identificarea bunelor practici ce permit atingerea unui nivel optim de securitate cibernetică și care pot fi preluate de către state.

Pentru a ilustra procesul de apariție, aplicare și validare a bunelor practici în domeniul securității cibernetice, articolul își propune să prezinte practica recurentă a raportării incidentelor ce afectează comunicațiile electronice, organizată de European Union Agency for Cybersecurity (ENISA), și rezultatele acesteia, însă nu înainte de a evidenția câteva aspecte care ne ajută să înțelegem relevanța bunelor practici.

1. Practicile organizațiilor internaționale

În literatura de specialitate, reticența statelor față de eficacitatea acțiunii organizațiilor internaționale este indicată ca fiind contextul în care practicile devin „o alegere pragmatică a acestora, din dorința de a-și proteja reputația prin implementarea unor dispozitive orientate către obținerea unor rezultate tangibile”[2]. Și Cornelia Navari consideră practicile ca fiind necesare pentru a asigura operaționalizarea principiilor care stau la baza instituțiilor internaționale: „Pentru a deveni o instituție a societății internaționale cu rol de organizare, în sensul stabilit de Holsti, este necesară tranziția de la principii constitutive la proceduri reglementate și practici recurente ale acestora, într-o perioadă lungă de timp”[3]. Aplicarea unor metodologii și controlul activităților determinate de aceasta poate avea ca rezultat colectarea de date legate de fenomenul care face obiectul acestor practici și care pot servi ulterior formulării unor recomandări de acțiune diferențiată. Mai mult, practicile din cadrul organizațiilor internaționale pot avea ca efect ameliorarea calității statisticilor și rapoartelor acestor instituții[4]. În domeniul securității cibernetice, acest ultim aspect este deosebit de relevant, dată fiind noutatea acestui domeniu și nevoia de „cooperare, coordonare, mecanisme formale și informale de colaborare, precum și mecanisme pentru rutinarea comportamentului internațional al statelor”[5].

La nivel conceptual, Nazli Choucri consideră instituționalismul ca fiind una dintre teoriile care poate oferi un cadru de abordare a securității cibernetice, cu mențiunea că sunt necesare anumite modificări ale cadrului teoretic. Pe de o parte, susține Choucri, teoriile tind să ignore „efectele răspuns și cele pe termen lung ale modificărilor pe termen scurt”[6]. Pe de altă parte, cadrul teoretic trebuie să ofere mecanisme de armonizare a interacțiunii dintre state și sectorul privat. Designul practicilor ENISA integrează cele două aspecte prin caracterul recurent al acțiunilor și prin implicarea furnizorilor de servicii în practicile de raportare a incidentelor. Perspectiva pe termen lung permite observarea rezultatelor tangibile obținute în urma aplicării unor astfel de practici în domeniul securității cibernetice, precum: stabilirea unor canale de comunicare eficientă între state, standardizarea procedurilor de comunicare, limitarea impactului incidentelor cibernetice, vizibilitate asupra infrastructurilor și crearea unui climat de încredere. În concluzie, bunele practici contribuie în mod direct la securitatea cibernetică a statelor și stabilirea unui cadru organizat pentru relațiile multilaterale.

În ciuda faptului că statele au la dispoziție o paletă largă de programe în domeniul securității cibernetice oferite de diferitele organizații internaționale, Choucri consideră totuși că există un decalaj între „cererea de gestionare a agendei globale și oferta de mecanisme de exercitare a autorității”[7]. Ea nu detaliază această afirmație, însă trebuie amintit că atingerea rezultatelor tangibile menționate anterior este condiționată de metodologiile care stau la baza practicilor dintre organizațiile internaționale și state.

2. Practica de raportare a incidentelor de securitate

Raportarea incidentelor ce afectează comunicațiile electronice organizată de ENISA are la bază prevederile Articolului 13a din Directiva 2009/140/CE[8] și este valoroasă din perspectiva următoarelor as-

---

[1] ***, *How to capture ad share your good practices in order to generate change?*, Food and Agriculture Organization of the United Nations, URL: http://fao.org/capacity-development/resources/practical-tools/good-practice-tool/en, accesat la 08.07.2020.

[2] Asmara Klein, Camille Laporte, Marie Saiget, “Introduction”, în Asmara Klein, Camille Laporte, Marie Saiget (dir.), *Les bonnes pratiques des organisations internationales*, Les Presses de Sciences Po, Paris, 2015, p. 25.

[3] Cornelia Navari, “Modelling the Relations of Fundamental Institutions and International Organizations”, în Tonny Brems Knudsen, Cornelia Navari (eds.), *International Organization in the Anarchical Society*, Palgrave Macmillan, 2019, p. 56.

[4] Benoît Martin, “Les quantifications dans l’expertise des organisations internationales. Le cas de l’UNODC” în Asmara Klein, Camille Laporte, Marie Saiget (dir.), *op. cit.*, 2015, p. 138.

[5] Nazli Choucri, *Cyberpolitics in International Relations*, The MIT Press, Cambridge, 2012, p. 15.

[6] *Ibidem*.

[7] *Ibidem*, p. 155.

[8] ***, *Directiva 2009/140/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivelor 2002/21/CE privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice, 2002/19/CE privind accesul la rețelele de comunicații electronice și la infrastructura asociată, precum și interconectarea acestora și 2002/20/CE privind autorizarea rețelelor și serviciilor de comunicații electronice*, Jurnalul Oficial al Uniunii Europene, nr. L 337, 18 decembrie 2009.

pecte:

➢ reprezintă o practică recurentă ce angajează diferite tipuri de actori;

➢ ilustrează procesul unei implementări pe termen lung, ceea ce face posibilă observarea efectelor pe care le produc practicile inițiate;

➢ are la bază o metodologie ce poate genera date despre activitatea statelor;

➢ prezintă posibile explicații pentru datele prezentate.

Conținutul documentului menționat prevede ca furnizorii de servicii și operatorii de rețele publice să raporteze autorităților naționale toate incidentele cu impact semnificativ, iar autoritățile naționale competente trebuie să informeze ENISA cu privire la orice incident cu impact transfrontalier. Statele trebuie, de asemenea, să prezinte un raport anual al incidentelor înregistrate.

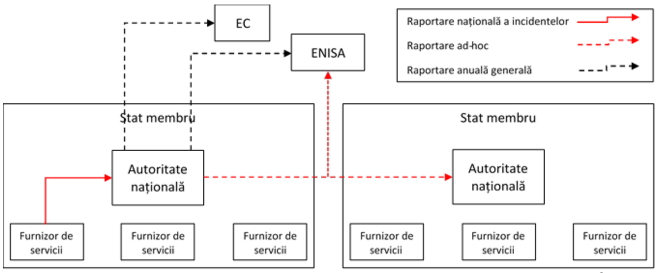


Figura nr. 1 - Procedura de raportare a incidentelor[9]

Începând cu anul 2010, ENISA menține o practică de raportare anuală a incidentelor cu impact semnificativ asupra comunicațiilor electronice, prevăzută de Articolul 13a din Directiva 2009/140/CE. Inițial, procedura se realiza prin e-mail, fiind înlocuită ulterior cu un program online. Criteriile de evaluare a incidentelor ce trebuie incluse în raport pot varia cu fiecare ediție, de aceea autorii recomandă o atenție sporită în stabilirea unor concluzii.[10] Potrivit rapoartelor, această practică recurentă are ca obiectiv asigurarea transparenței și stabilirea unui proces de învățare pe baza incidentelor înregistrate deja, cu scopul îmbunătățirii calității acestei practici, dar și a securității comunicațiilor electronice. Studiile realizate nu conțin detalii despre statele care au înregistrat incidente, ci doar informații legate de numărul total de incidente, servicii, număr de utilizatori, cauza incidentelor, tipul de echipament afectat. Raportul din 2018[11] a inclus și evaluarea multianuală a evoluției acestor indicatori pentru perioada 2012-2018.

Pentru a ajuta statele în implementarea conținutului normativ menționat, practica raportării incidentelor de securitate a fost însoțită și de un studiu ENISA asupra indicatorilor utilizați în raportarea incidentelor de securitate[12]. Printre obiectivele acestui studiu se numără asistarea statelor în măsurarea impactului incidentelor de securitate, cartografierea indicatorilor utilizați de autoritățile naționale și furnizorii de servicii, dar și sublinierea diferențelor de abordare între acești actori. La toate acestea, se adaugă și ambiguitatea normativă: „Faptul că autoritățile naționale s-au confruntat cu o confuzie în definirea, identificarea și măsurarea acurată a indicatorilor incidentelor de securitate poate fi atribuit, în mare parte, ambiguității conținute de Articolul 13a. Acesta prevede ca autoritățile naționale și furnizorii de servicii trebuie să adopte pașii potriviți pentru a garanta integritatea rețelelor, dar nu specifică ce înseamnă „pași potriviți" și nici nu definește „integritatea". Nici detalii privind definirea relevanței unui incident nu sunt prevăzute în cadrul acestei Directive"[13].

Potrivit studiului elaborat de specialiștii ENISA, practica de analiză și identificare a indicatorilor a avut un impact pozitiv: 38% dintre autoritățile naționale au declarat că analiza indicatorilor a ajutat la concretizarea unor proceduri mai bune de evaluare a riscului la nivel național, iar 46% dintre autoritățile naționale au fost de acord că analiza indicatorilor a contribuit la o mai bună securitate la nivel național[14]. Cercetarea realizată de grupul de lucru ENISA a evidențiat și abilitatea acestei instituții de a furniza o metodă de determinare a caracterului critic al incidentelor: "când caracterul critic a fost luat în considerare, pentru cea mai mare parte, aproape toți respondenții au utilizat metrica ENISA"[15]. Aceste date evidențiază, pe de o parte, procesul de validare a practicilor inițiate de organizațiile internaționale, în urma aplicării lor de către state, iar, pe de altă parte, contribuția organizațiilor internaționale prin acțiuni specifice (spre exemplu, identificarea unor indicatori) la sporirea gradului de securitate cibernetică. Efectele benefice resimțite de state confirmă rolul coordonator și legitimitatea organizațiilor internaționale.

3. Rezultatele practicii de raportare a incidentelor de securitate

După cum am menționat, raportul ENISA pentru anul 2018 prezintă evoluția multianuală a acestor indicatori ai incidentelor de securitate pentru perioada 2012-2018, ceea ce legitimează calitatea statisticilor oferite de această instituție. După cum se poate observa în figura nr. 2, principala sursă de incidente ce afectează statele sunt avariile de

---

[9] Aggelos Koukounas, Eleni Vytogianni, Marnix Dekker, *Annual report telecom security incidents 2018*, ENISA, May 2019, p. 7.

[10] ***, *Annual Incident Reports 2015: Analysis of Article 13a annual incident reports in the telecom sector*, ENISA, September 2016, p. 12.

[11] Aggelos Koukounas, Eleni Vytogianni, Marnix Dekker, *op. cit.*, May 2019.

[12] Dan Tofan, Konstantinos Moulinos, Christoffer Karsberg, *Security incidents indicators – measuring the impact of incidents affecting electronic communications*, ENISA, 2015.

13 *Ibidem*, p. 10.

14 *Ibidem*, p. 11.

15 *Ibidem*, p. 40.

sistem, înregistrând o diferență superioară față de alte posibile cauze precum erorile umane, fenomenele naturale și acțiunile ostile. Acest tip de statistică ajută statele să înțeleagă diferitele fațete ale securității cibernetice naționale. De asemenea, aceste rezultate legitimează poziția ENISA de a considera incidentele de securitate în funcție de efectul pe care îl produc – întreruperea serviciilor către utilizatori – și nu în funcție de sursa acestora.

Prin stabilirea unor canale de comunicare de durată, ENISA face ca această abordare să fie transferată în practica statelor și a operatorilor de infrastructuri de telecomunicații. Procedura de raportare a incidentelor prevede stabilirea unor canale de comunicare la nivel național, între operatorii de servicii și autoritățile naționale, și la nivel internațional, între autoritățile naționale și instituția ce coordonează și colectează datele rezultate din aceste schimburi. Agenția europeană instituie astfel un perimetru de colaborare bine definit între state, atât de necesar cooperării internaționale. Mai mult, utilizarea unor categorii comune face ca interacțiunea dintre state să se raporteze la același sistem de referință, care consolidează înțelegerea comună a provocărilor de securitate cibernetică.

Prin cunoașterea aprofundată a provocărilor și a riscurilor, practica raportării incidentelor contribuie la stabilirea unei agende naționale de securitate cu caracter inclusiv. În concluziile raportului ENISA pentru anul 2018, se menționează faptul că practica raportării incidentelor a generat informații utile pentru factorii de decizie politică. Mai mult, acest raport confirmă sintagma „bune practici” prin efectele sale în materie de standardizare: „În particular, definiția incidentului de securitate și definiția limitelor pentru emiterea unei notificări sunt perfect integrate. Ceea ce înseamnă că există o oportunitate clară de armonizare a taxonomiei, proceselor și instrumentelor. ENISA sprijină procesul de identificare și exploatare a acestor sinergii, spre exemplu prin utilizarea aceleiași taxonomii de cauze a incidentelor”[16].

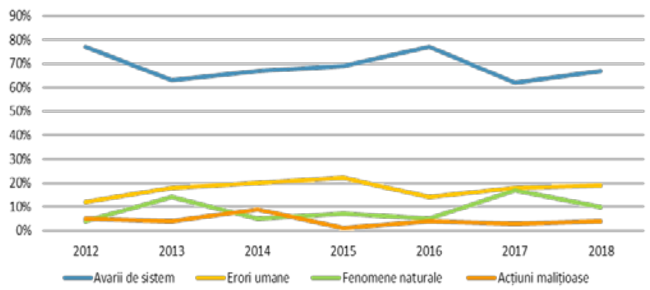


Figura nr. 2 - Categorii de cauze ale incidentelor de securitate în sectorul Telecom din UE raportate în perioada 2012-2018[17]

După cum este prezentat în raportul ENISA și se poate observa în figura nr. 2, se înregistrează o creștere a impactului pe care îl au fenomenele naturale asupra serviciilor de telecomunicații. În ceea ce privește atacurile cibernetice și erorile umane, impactul se menține constant pe perioada celor șapte ani de raportare.

Începând cu anul 2017, se constată o tendință de scădere a procentului de ore pierdute din cauza avariilor înregistrate de elementele hardware și software, depășit acum de efectele fenomenelor naturale (figura nr. 3).

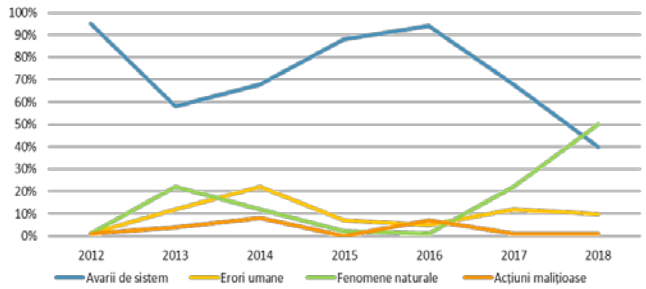


Figura nr. 3 - Impactul incidentelor exprimat în numărul total de ore pierdute de către utilizatori, în funcție de cauzele incidentelor[18]

Pe durata perioadei de raportare, ENISA a înregistrat un total de 940 de incidente, din care 4% au fost generate de atacuri cibernetice. Figura de mai jos arată evoluția incidentelor și a impactului acestora pe parcursul celor șapte ani, în ultimul an înregistrându-se o scădere a orelor pierdute de utilizatori. Raportul avansează posibile cauze ale acestei tendințe, precum modificările la nivelul infrastructurii de rețea, dar urmărește clarificarea acestui aspect prin comparație cu rezultatele următoarelor rapoarte, ceea ce consolidează recurența ca aspect esențial al practicilor. În general, rapoartele ENISA corelează datele și tendințele prezentate cu posibile explicații, ceea ce consolidează legitimitatea acestei instituții internaționale în măsură de cunoaștere a fenomenului urmărit – securitatea cibernetică.

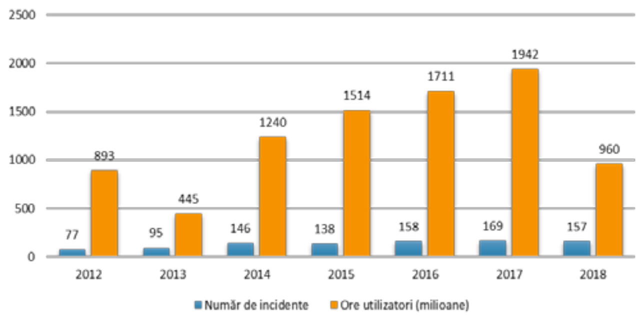


Figura nr. 4 - Raportul multianual privind numărul de incidente și orele pierdute de către utilizatori[19]

4. România și practica de raportare a incidentelor

[16] Aggelos Koukounas, Eleni Vytogianni, Marnix Dekker, *op. cit.*, May 2019, p. 17.
[17] *Ibidem*, p. 14.
[18] *Ibidem*, p. 15.
[19] *Ibidem*, p. 16.

România este unul dintre statele care aplică practica de raportare a incidentelor către ENISA, obligativitatea fiind prevăzută de Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice[20]. Urmând schema de raportare prezentată în primul capitol, furnizorii de servicii și operatorii de rețele publice trebuie să raporteze către Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM) incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice. ANCOM pune la dispoziția furnizorilor de servicii chestionare care ajută la evaluarea impactului, duratei și cauzei incidentelor.

Potrivit Raportului privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2019 al Autorității Naționale pentru Administrare și Reglementare în Comunicații, un număr de doar 11 incidente s-au încadrat în categoria care trebuie raportată la ENISA, dintr-un total de 794 raportate la nivel național[21]. Aceste rapoarte sunt prezentate pe pagina oficială ANCOM, începând cu anul de raportare 2011. Trebuie menționat că furnizorii de servicii au la dispoziție instrucțiuni și un formular standard pentru evaluarea incidentelor, iar obiectul raportării este delimitat la incidentele cu impact semnificativ, respectiv care afectează un număr mai mare de 5.000 de conexiuni, timp de cel puțin 60 de minute.

Concluzii

Punctul de plecare în scrierea acestui text a fost identificarea mecanismelor care stau la baza constituirii bunelor practici în domeniul securității cibernetice. Activitatea ENISA ilustrează modalitatea prin care practicile din cadrul organizațiilor internaționale sunt transferate, puse în aplicare, evaluate și validate ca bune practici de către state. Acestea sunt asistate în implementarea prevederilor din cadrul actelor normative prin intermediul acestor practici, iar datele generate din interacțiunea dintre state și instituțiile din cadrul organizațiilor internaționale îmbunătățesc calitatea statisticilor. Practicile ENISA sunt scrise pe „palimpsestul" teoriei organizațiilor internaționale, rezultatele confirmând capacitatea acestei instituții de a iniția modificări în domeniul securității cibernetice și de a colecta date privind efectele acestora pe termen lung.

Raportarea incidentelor de securitate reprezintă o modalitatea de a reduce complexitatea conceptului de securitate cibernetică la categorii și unități observabile, precum incidentele de securitate și cauzele acestora, și de a constitui o referință comună pentru state. Datele generate de studiile ENISA contribuie la crearea unui cadru fiabil de cooperare, bazat pe cunoașterea reciprocă dintre state, și a unui climat de încredere. Cooperarea între state, în cadrul ENISA, este favorizată, printre altele, de decizia de a nu include detalii despre statele care au înregistrat incidente.

Nu în ultimul rând, raportul direct dintre aplicarea practicilor și standardizare, aspect confirmat de rezultatele pe termen lung ale implementării practicilor ENISA, poate deveni o temă viitoare de cercetare din perspectiva analizei condițiilor de apariție a rezultatelor și a variabilității acestora.

Bibliografie:

1. CHOUCRI, Nazli, *Cyberpolitics in International Relations*, The MIT Press, Cambridge, 2012.
2. KLEIN, Asmara; Camille LAPORTE, Marie SAIGET, "Introduction", în Asmara KLEIN, Camille LAPORTE, Marie SAIGET (dir.), *Les bonnes pratiques des organisations internationales*, Les Presses de Sciences Po, Paris, 2015.
3. KOUKOUNAS, Aggelos; Eleni VYTOGIANNI, Marnix DEKKER, *Annual report telecom security incidents 2018*, ENISA, May 2019.
4. MARTIN, Benoît, "Les quantifications dans l'expertise des organisations internationales. Le cas de l'UNODC" în Asmara KLEIN, Camille LAPORTE, Marie SAIGET (dir.), *Les bonnes pratiques des organisations internationales*, Les Presses de Sciences Po, Paris, 2015.
5. NAVARI, Cornelia, "Modelling the Relations of Fundamental Institutions and International Organizations", în Tonny Brems KNUDSEN, Cornelia NAVARI (eds.), *International Organization in the Anarchical Society*, Palgrave Macmillan, 2019.
6. TOFAN, Dan; Konstantinos MOULINOS, Christoffer KARSBERG, *Security incidents indicators – measuring the impact of incidents affecting electronic communications*, ENISA, 2015.
7. ***, *Annual Incident Reports 2015: Analysis of Article 13a annual incident reports in the telecom sector*, ENISA, September 2016.
8. ***, *Directiva 2009/140/CE a Parlamentului European și a Consiliului din 25 noiembrie 2009 de modificare a Directivelor 2002/21/CE privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice, 2002/19/CE privind accesul la rețelele de comunicații electronice și la infrastructura asociată, precum și interconectarea acestora și 2002/20/CE privind autorizarea rețelelor și serviciilor de comunicații electronice*, Jurnalul Oficial al Uniunii Europene, nr. L 337, 18 decembrie 2009.
9. ***, *How to capture ad share your good practices in order to generate change?*, Food and Agriculture Organization of the United Nations, URL: http://fao.org/

[20] ***, *Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare*, URL: http://www.ancom.org.ro/uploads/articles/file/legislatie/OUG%202011_111.pdf, accesat la 20.07.2020.

[21] ***, *Raport privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2019*, Autoritatea Naţională pentru Administrare și Reglementare în Comunicații, iunie 2020, URL: https://www.ancom.ro/uploads/links_files/Raport_incidente_2019.pdf, accesat la 03.08.2020.

capacity-development/resources/practical-tools/good-practice-tool/en.

10. ***, *Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată cu modificări și completări prin Legea nr. 140/2012, cu modificările și completările ulterioare*, URL: http://www.ancom.org.ro/uploads/articles/file/legislatie/OUG%202011_111.pdf.
11. ***, *Raport privind incidentele care au afectat securitatea și integritatea rețelelor și serviciilor de comunicații electronice în anul 2019*, Autoritatea Naţională pentru Administrare și Reglementare în Comunicații, iunie 2020, URL: https://www.ancom.ro/uploads/links_files/Raport_incidente_2019.pdf.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 1155/2020

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro